



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/424,685	01/11/2000	TERUHIKO TAMORI	16966-00002	8381

7590 07/11/2003

ALAN L CASSEL
ARMSTRONG TEASDALE
ONE METROPOLITAN SQUARE
SUITE 2600
ST LOUIS, MO 63102

EXAMINER

YANG, CLARA I

ART UNIT

PAPER NUMBER

2635

DATE MAILED: 07/11/2003

17

Please find below and/or attached an Office communication concerning this application or proceeding.

B

Office Action Summary

Application No.

09/424,685

Applicant(s)

TAMORI, TERUHIKO

Examiner

Clara Yang

Art Unit

2635

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 May 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3,6,7,9,10,13-16,18-20,22-25,27 and 28 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

- 5) ☐ Claim(s) _____ is/are allowed.

- 6) ☒ Claim(s) 1-3,6,7,9,10,13-16,18-20,22-25,27 and 28 is/are rejected.

- 7) ☐ Claim(s) _____ is/are objected to.

- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____. 6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed on 23 May 2003 with respect to claims 1 - 3, 6, 7, 9, 10, 13 - 16, 18, 19, 20, 22 - 24, 27, and 28 have been considered but are moot in view of the new ground(s) of rejection.
2. Applicant's arguments filed on 23 May 2003 with respect to claims 9, 10, 18, 19, and 25 have been fully considered but they are not persuasive.

In response to the Applicant's request that 35 USC § 112, first paragraph, rejections of claims 9, 10, and 18 be withdrawn, the amendment of these claims fails to overcome the rejection. Consequently, the Examiner maintains the 35 USC § 112, first paragraph, rejections of claims 9, 10, and 18.

Regarding Claim 25, in response to applicant's argument on pages 17 - 18 that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, both Scott and Borza teach devices that prevent unauthorized use of a vehicle. Scott's fingerprint recognition transmitter 10 is used to transmit a fingerprint image (see Col. 3, lines 41 - 53). Upon authorization, an individual uses transmitter 10 to open the vehicle's door(s), start the engine, etc. (see Col. 3, lines 53 - 64). Scott is silent on the step of limiting vehicular speed in accordance with a matched registered driver. Borza's method of preventing unauthorized use of a vehicle includes the steps of: (a) getting a

Art Unit: 2635

fingerprint; (b) comparing the received fingerprint with the registered fingerprint; and (c) repeating the verification if the comparison is false or allowing normal operation of the vehicle if the comparison is true. Borza's method further allows a permanent user to limit the fuel flow rate to a predetermined maximum when a temporary user accesses the vehicle, thus limiting the vehicle's speed in accordance with data stored in NVM 16d for that temporary user (see Col. 5, lines 10 - 6 and Col. 6, lines 4 - 9). By modifying Scott's system as taught by Borza, in addition to preventing unauthorized entry and starting of the vehicle, a vehicle owner is able to prevent temporary users from abusing the vehicle by limiting the speed of the vehicle.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 9, 10, 18, and 19 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter that was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claims 9 and 10, the limitation "a slot for insertion of an information recording/processing device, said slot comprising an external terminal configured to mate with an exposed terminal of the information recording/processing device, said external terminal being where data is passed to said control device, the data being at least fingerprint data from a user of the information recording/processing device" is considered to be new matter. Claims 9

Art Unit: 2635

and 10 recite a *machine/system control device*, which is understood to be the second embodiment of the Applicant's invention and is supported in Figs. 4 - 6 and pages 12 - 17. On page 12, the Applicant discloses that Fig. 4 is a conceptual diagram of a car driving system that is a machine/system control device. As taught by the Applicant (see pages 13 - 14 and Fig. 5), the machine/system control device comprises a remote controller 3 (i.e., the information recording/processing device) that has a fingerprint sensor module 31 and an infrared (IR) transmission unit 33 for sending detected fingerprint data to receiver unit 4 of the vehicle. The Applicant omits teaching a machine/system control device wherein the vehicle system comprises "a slot for insertion" of remote controller 3. In addition, the Applicant omits teaching in the specification that remote controller 3 has an external terminal. On page 15, the Applicant clearly expresses that IR transmission unit 33, not an external terminal, is used to pass data to the vehicle's control mechanism.

Regarding claim 18, the limitation "user-specific information is fingerprint data from a person who has authority to inspect or rewrite information in the information recording/processing device" is considered to be new matter. Claim 18 is dependent on claim 9, which recites a *machine/system control device*. The Applicant omits teaching that (1) user-specific information is fingerprint data and (2) that the fingerprint data must be from "a person who has authority to inspect or rewrite information" in remote controller 3 or the information recording/processing device. In fact, the Applicant differentiates between fingerprint data and user-specific information. On page 14, the Applicant imparts that "name, sex, age, license number, category of the license, upper speed limit, etc." are examples of user-specific information and are stored in personal information memory 43, whereas fingerprint data is stored in fingerprint register memory 41. Furthermore, the Applicant only specifies that the

Art Unit: 2635

fingerprint register memory 41 stores fingerprints of authorized drivers, not "a person who has authority to inspect or rewrite information in the information recording/processing device."

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1 – 3, 13 – 16, 27, and 28 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 4,582,985 (Löfberg).

Referring to Claims 1 – 3, a block diagram of Löfberg's data carrier 1, which is shaped as a credit card, is shown in Fig. 1 (see Abstract). As shown in Fig. 1, Löfberg's data carrier 1 comprises: (a) sensor device 2 for obtaining fingerprint information of the user (see Abstract; Col. 4, lines 31 – 35); (b) reading means 3 and signal processing device 4 that form a conversion unit for converting the fingerprint data detected by sensor device 2 into binary information (i.e., digital electrical signals) (see Col. 4, lines 38 – 53); and (c) a block 7 that includes a switching means for establishing a signal path to enable an exchange of data between the data carrier and a terminal equipment (see Col. 5, lines 41 – 44). Because Löfberg's data carrier 1 is an active data card and Löfberg discloses that active data cards are provided with a number of externally available electrical connection means or corresponding coupling means for communication with

Art Unit: 2635

a terminal (see Col. 1, lines 42 - 45), it is implied that block 7 has an exposed electrical terminal. Löfberg's data carrier 1 further comprises: (d) memory 6 for storing fingerprint data as a reference bit sequence or registered fingerprint data (see Col. 4, lines 55 - 60 and Col. 8, lines 49 - 58); and (e) comparator 5 for comparing newly detected fingerprint data with the registered fingerprint data stored in memory 6 and to output a signal indicative of when there is a match of the fingerprints in the comparison to the exposed terminal (see Col. 4, lines 55 - 60; Col. 5, lines 30 - 44; and Col. 12, lines 40 - 60).

Regarding Claims 13 and 14, Löfberg teaches that the data carrier holds information about the owner of the data carrier, account number, etc., (see Abstract and Col. 12, lines 51 - 56). Because memory 6 stores the registered fingerprint data and the various scanning methods (see Col. 10, lines 38 - 42 and Col. 12, lines 8 - 16), it is understood that a second memory unit stores the specific information about the owner of the data carrier.

Regarding Claims 15 and 16, Löfberg's sensor device 2 is formed by a matrix 9 of sensing surfaces 9', wherein each sensing surface 9' comprises of two plates (see Fig. 1). Because Löfberg's sensor device 2 detects a user's fingerprint line pattern when the user's finger ridges causes the current path to closed between the two plates, such as plates 21 and 22 in Fig. 2 or plates 30 and 32 (see Col. 5, lines 66 - 68; Col. 6, lines 1 - 68; and Col. 7, lines 1 - 7), Löfberg's sensor device 2 is understood to be a surface pressure input type sensor.

Referring to Claims 27 and 28, Löfberg method for authentication comprises the following steps: (a) recording the owner's fingerprint via sensor device 2 of data carrier 1 (see Fig. 1) and storing the resulting reference bit sequence in memory 6 (see Col. 8, lines 49 - 54); (b) sensing a fingerprint of the owner via sensor device 2 (see Col. 4, lines 31 - 53 and Col. 8, lines 54 - 58); (c) comparing the sensed fingerprint of the owner to the registered fingerprint data

Art Unit: 2635

using comparator 5 (see Col. 4, lines 54 - 60); (d) generating an acceptance signal by comparator 5 that is indicative of a match of the sensed fingerprint data and the registered fingerprint data (see Col. 5, lines 30 - 34 and Col. 12, lines 17 - 20); and (e) outputting a result of the comparison to an exposed terminal of data carrier 1's block 7, wherein the exposed terminal is configured for electrical connection with an external terminal (see Col. 1, lines 42 - 45; Col. 5, lines 41 - 44; and Col. 12, lines 40 - 60).

7. Claims 1 - 3, 15, 16, and 27 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,180,901 (Hiramatsu).

Referring to Claims 1 - 3, Hiramatsu teaches an integrated circuit (IC) card with authentication function. As shown in Figs. 1 and 3, Hiramatsu's IC card comprises: (a) pressure sensor 1 or fingerprint sensor (see Col. 2, lines 56 - 62 and Col. 5, lines 21 - 58); (b) analog/digital (A/D) converter 2 for converting fingerprint data detected by pressure sensor 1 into digital signals (see Col. 4, lines 57 - 60); (c) external connection contact 11 for connection to an external system, such as an automated teller machine (ATM) terminal (see Col. 4, lines 20 - 21 and 43 - 49); (d) dictionary memory 7 for storing fingerprint data sensed by pressure sensor 1 as registered fingerprint data (see Fig. 9; Col. 7, lines 51 - 68; and Col. 8, lines 1 - 4); and (e) controller 8 or fingerprint matching unit (see Col. 5, lines 2 - 20). Hiramatsu imparts in Col. 4, lines 43 - 49, that an ATM terminal receiving the IC card executes normal operation commands if the card is authenticated (i.e., finger characteristics stored in image memory 7 and dictionary memory 7 coincide with each other), thus implying that the IC card must transmit a signal to the ATM machine indicating whether there is a match or not via external connection contact 11.

Regarding Claims 15 and 16, Hiramatsu teaches inputting fingerprint data into an IC card via pressure sensor 1 (see Col. 2, lines 56 - 62 and Col. 5, lines 21 - 58).

Referring to Claim 27, Hiramatsu's method comprises the following steps: (a) inputting the owner's fingerprint data via pressure sensor 1 and storing the resulting sum signal 20 in dictionary memory 7 (see Fig. 9; Col. 7, lines 51 - 68; and Col. 8, lines 1 - 4); (b) sensing a fingerprint via pressure sensor 1 (see Fig. 11, ST6; Col. 4, lines 57 - 60; and Col. 8, lines 15 - 19); (c) comparing the sensed fingerprint to the registered fingerprint data in dictionary memory 7 (see Fig. 11, ST9 and ST10; Col. 5, lines 9 - 12; and Col. 8, lines 23 - 26); and (d) outputting a result of the comparison to microprocessor 9, thus enabling the IC card to exchange information with an ATM terminal and implying that the IC card must transmit a signal to the ATM machine indicating that there is a match via external connection contact 11 (see Col. 5, lines 12 - 20 and Col. 9, lines 18 - 24).

8. Claims 9, 10, 18, and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,987,155 (Dunn et al.).

Referring to Claims 9 and 10, Dunn teaches a biometric input device 20 (see Fig. 2) that is connected to a computer. Here it is understood that biometric input device 20 and the computer to which it is connected to form a machine/system control device. Dunn's machine/system control device comprises: (a) contact imaging device 21 or fingerprint sensor (see Col. 7, lines 4 - 5); (b) a memory in the computer connected to biometric input device 20 for storing registered fingerprint data (see Col. 7, lines 32 - 47 and Col. 8, lines 51 - 54); (c) a fingerprint matching unit (see Col. 7, lines 39 - 47); (d) a control mechanism configured to control operation of the machine/system control device in accordance with user-specific information corresponding to the fingerprint (such as setting up user preferences) when there is a match with the registered fingerprint data (see Col. 7, lines 36 - 42); and (e) slot 23 for receiving smart card 25, wherein slot 23 has a peripheral card interface or an external terminal

Art Unit: 2635

for mating with smart card 25 (see Col. 7, lines 28 - 30). Dunn also teaches that when a user inserts smart card 25 into slot 23 and provides a fingerprint to contact imaging device 21, the biometric information is converted into an electrical signal and provided to the smart card (see Col. 7, lines 28 - 33). Using an algorithm specified by the user, smart card 25 processes the electrical signal and provides the processed information to the peripheral card interface, which sends the processed information via a data transfer means to the computer for comparison with registered fingerprint data (see Col. 7, lines 33 - 47 and Col. 8, lines 19 - 29).

Regarding Claim 18, Dunn imparts that a user can have several smart cards for different applications, such as for voice processing and filtering (see Col. 6, lines 8 - 40), and that each smart card 25 is password protected or protected by an alternative form of biometric information and able to be modified (see Col. 6, lines 65 - 67 and Col. 7, lines 1 - 2). Here it is understood that the owner of smart card 25 is able to modify smart card 25.

Regarding Claim 19, Dunn's contact imaging device 21 a capacitive fingerprint imager, thus implying that imaging device 21 is a surface pressure input type fingerprint sensor.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 6, 7, 20, and 22 - 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,565,000 (Sehr) in view of U.S. Patent No. 5,559,504 (Itsumi et al.).

Referring to Claim 6, Sehr teaches a passenger card 11 or portable information recording unit that comprises database storage means, processing and communications capabilities, and display means (see Col. 6, lines 27 - 29). Sehr imparts that a passenger can use biometric box 13 of card station 1 (as shown in Fig. 1) to capture and digitize his/her biometric information, such as fingerprint, and use card reader 12 to write the captured biometric information to card 11 (see Col. 6, lines 45 - 67), thus implying that card 11 has at least a first memory unit for storing fingerprint data detected by biometrics box 13. Furthermore, as shown in Fig. 3, Sehr discloses the contents stored in card 11, which include the passenger's name, address, birth date, etc. (see Col. 14, lines 24 - 31). Here it is understood that a second memory unit stores the passenger-specific information. Sehr also teaches multiple control modules or information processing units (see Fig. 1, card station 1). Card station 1 comprises: (a) card reader/writer 12 for interfacing with card 11 (see Col. 6, lines 45 - 50); (b) biometrics box 13 for capturing and digitizing fingerprints, voice, signature, etc. (see Col. 6, lines 58 - 67); (c) biometrics matching unit configured to compare newly detected fingerprint or signature data received at biometrics box 13 with the registered fingerprint or signature data stored on card 11 (see Col. 13, lines 9 - 16 and see Col. 34, lines 32 - 35); (d) database 10 or third memory unit for storing biometrics data captured and digitized by biometrics box 13 (see Col. 6, lines 61 - 63); and (e) a display (see Col. 6, lines 48 - 50). Here it is understood that biometrics box 13 includes a thin fingerprint sensor. Sehr's card 11 lacks a thin fingerprint sensor and an exposed terminal configured for connecting with a control module's card reader/writer 12. In addition, Sehr omits teaching that card reader/writer 12 has an external terminal configured for connecting with the external terminal of card 11.

In an analogous art, Itsumi's IC card 63 or portable information recording unit, as shown in Fig. 26, comprises: (a) fingerprint input unit 70 or thin fingerprint sensor; (b) fingerprint data registration memory 74; (c) information recording memory 75, which is understood to be a memory for storing user-specific information; and (d) external terminal 76 for inputting and outputting information from and to an external terminal of an information processing unit, such as a banking system or the like. (See Col. 15, lines 14 - 36). Itsumi teaches that the information processing unit has an external terminal for exchanging information with IC card 63 via external terminal 76 of IC card 63 (see Col. 15, lines 32 - 36).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify card 11 and card reader/writer 12 of Sehr as taught by Itsumi because (1) external terminals are effective and well-known means for connecting devices, and (2) a self-authenticating card 11 determines that the person who currently inputs the fingerprint is the lawful bearer before card 11 is rendered operable (see Itsumi, Col. 15, lines 28 - 36), thus preventing unlawful use of the card and enhancing the security of the system.

Regarding Claim 7, by using card reader/writer 12 of card station 1, a passenger can read from, write to, and rewrite information stored on card 11 (see Col. 6, lines 45 - 57; Col. 13, lines 43 - 56; and Col. 14, lines 55 - 51).

Referring to Claim 20, one of Sehr's methods comprises the steps of: (a) an airline representative (a first person) coupling a passenger's (a second person) card 11 to a control module (see Col. 34, lines 14 - 16); (b) the control module reading identification data from (see Col. 34, lines 16 - 28); (d) the airline representative requesting additional information to further verify the lawful bearer, such as the passenger's signature that is entered via a signature pad or biometrics box 13 (see Col. 34, lines 28 - 32); and (e) the control module comparing the obtained

Art Unit: 2635

additional information to the information read from card 11 (see Col. 34, lines 32 - 35). Because Sehr expresses that biometrics box 13 includes means for capturing and digitizing fingerprints (see Col. 6, lines 58 - 61), it is understood that a passenger's fingerprints can also be used to verify the passenger. Sehr omits teaching the following steps: (a) registering fingerprint data of the airline representative; (b) pressing a finger of the airline representative on a fingerprint sensor of the control module; and (c) allowing access to card 11's database when the airline representative's fingerprint matches the registered fingerprint in database 10 of the control module. However, the Examiner takes Official Notice that the use of biometric sensors to prevent unauthorized access to databases and the method of registering authorized users' fingerprints and allowing verified users to access the databases are well known. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to add the above mentioned steps to Sehr's method since the Examiner takes Official Notice that such modifications are well known and will prevent unauthorized users from accessing sensitive data, thus improving the security of the system.

Regarding Claims 22 and 23, Sehr discloses an airline representative asking a passenger about luggage items that need to be checked in after successful verification, thus implying that the control module provides an indication of a successful verification to the airline representative. Because the control module is able to display card 11's information, such as the passenger's passport information (see Col. 34, lines 26 - 28), it is understood that control module provides a visual indication of a successful verification.

Regarding Claim 24, Sehr imparts that upon successful verification, the control module compiles and loads the boarding pass into the card and cancels the ticket portion that is related to the flight segment(s) the passenger has been qualified for (see Col. 34, lines 36 - 39).

Art Unit: 2635

11. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. U.S. Patent No. 6,111,977 in view of Borza U.S. Patent No. 5,867,802.

Scott's method of controlling access to a vehicle comprises the steps of placing a finger on a fingerprint sensor module of a remote control module, transmitting minutiae data of the fingerprint to a receiver mounted in the vehicle, comparing the minutiae data to data stored in a database of registered drivers, and conditioning the vehicle to unlock the door upon a match of the minutiae data to data stored in the database of registered drivers (see Col. 2, lines 16 - 39). Scott is silent on the step of limiting vehicular speed in accordance with a matched registered driver.

In an analogous art, Borza's method of preventing unauthorized use of a vehicle includes the step of allowing a permanent user to limit the fuel flow rate to a predetermined maximum when a temporary user accesses the vehicle, thus limiting the vehicle's speed in accordance with data stored in NVM 16d for that temporary user (see Col. 5, lines 10 - 6 and Col. 6, lines 4 - 9). Because Borza teaches that a permanent user can add temporary users to the system and that biometric data of temporary users are stored in memory 16d, it is understood that temporary users, in addition to a permanent user, are registered drivers.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method of Scott as taught by Borza because the step of restricting a registered temporary user's access to particular vehicle functions, in addition to preventing unauthorized entry and starting of the vehicle, enables the vehicle owner to prevent abuse of the car caused by excessive speed.


Art Unit: 2635

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Clara Yang whose telephone number is (703) 305-4086. The examiner can normally be reached on 8:30 AM - 7:00 PM, Monday - Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on (703) 305-4704. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 872-9314 for regular communications and (703) 872-9315 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4700.

CY
July 10, 2003



BRIAN ZIMMERMAN
PRIMARY EXAMINER